федеральное государственное бюджетное образовательное учреждение высшего образования "Приволжский исследовательский медицинский университет" Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Богомолова Е.С.
«25» мая 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине **Защита информации в медицинской организации**

направление подготовки **09.04.02 Информационные системы и технологии**

профиль **Информационные системы и технологии в здравоохранении**

Квалификация выпускника:
Магистр

Форма обучения:
очно-заочная

Нижний Новгород
2021

Фонд оценочных средств по дисциплине «Защита информации в медицинской организации» предназначен для контроля знаний по программе магистратуры по направлению подготовки 09.04.02 «Информационные системы и технологии», профилю «Информационные системы и технологии в здравоохранении».

1. Паспорт фонда оценочных средств по дисциплине «Защита информации в медицинской организации»

Компетенция	Результаты обучения	Виды занятий	Оценочные средства
ПК-2	способен разрабатывать и управлять проектной и программной документацией в области информационных систем		
	Знать: ИД-7$_{ПК-2.7}$ законодательство Российской Федерации в области защиты информации; **Уметь**: ИД-15$_{ПК-2.15}$ настраивать политику безопасности современных операционных систем на основе проектной и программной документации. **Владеть**: ИД-23$_{ПК-2.23}$ прикладными и инструментальными средствами создания систем информационной безопасности.	лекции, самостоятельная работа, семинары	Реферат, Собеседование
ПК-7	способен обеспечивать бесперебойную работу сети, создавать необходимое резервирование сетей и инфокоммуникаций, вносить предложения по их развитию и совершенствованию		
	Знать: ИД-4$_{ПК-7.4}$ особенности обеспечения информационной безопасности в компьютерных сетях и специфику средств защиты компьютерных сетей в медицинской организации. **Уметь**: ИД-8$_{ПК-7.8}$ применять компьютерные технологии для решения задач обеспечения защиты информации в медицинском учреждении. **Владеть**: ИД-12$_{ПК-7.12}$ методами использования компьютерных технологий для решения задач обеспечения защиты информации в медицинском учреждении.	лекции, самостоятельная работа, семинары	Реферат, Собеседование

Текущий контроль по дисциплине «Защита информации в медицинской организации» осуществляется в течение всего срока освоения данной дисциплины. Выбор оценочного средства для проведения текущего контроля на усмотрение преподавателя.

Промежуточная аттестация обучающихся по дисциплине «Защита информации в медицинской организации» проводится по итогам обучения и является обязательной.

2. Критерии и шкала оценивания

Индикаторы компетенции	*Критерии оценивания*	
	Не зачтено	*Зачтено*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Могут быть допущены несущественные ошибки
Наличие умений	Не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены все задания. Могут быть допущены несущественные ошибки.
Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач. Могут быть допущены несущественные ошибки.
Мотивация (личностное отношение)	Учебная активность и мотивация слабо выражены, готовность решать поставленные задачи качественно отсутствуют	Проявляется учебная активность и мотивация, демонстрируется готовность выполнять поставленные задачи.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Средний/высокий

3. Оценочные средства

3.1. Текущий контроль

3.1.1. Контролируемый раздел дисциплины «Методы и способы защиты информации от потери, искажения, подлога и несанкционированного копирования»

Темы рефератов

1). Модели нарушителей безопасности информации в медицинской организации.
2). Законодательная защита информации в медицинском учреждении РФ.
3). Мировой опыт в законодательной защите информации в медицине.
4). Предполагаемые последствия от потери, искажения, подлога и несанкционированного копирования медицинской информации.
5). Обзор методов и способов защиты информации от потери.
6). Обзор методов и способов защиты информации от искажения
7). Обзор методов и способов защиты информации от подлога.
8). Обзор методов и способов защиты информации от несанкционированного копирования.
9). Особенности медицинской информации, подлежащей защите.
10). Защита данных при обмене информацией между медицинскими организациями.

3.1.2. Контролируемый раздел дисциплины «Особенности обеспечения информационной безопасности в медицинской организации на аппаратном уровне»

Темы рефератов

1). Работоспособность персонального компьютера в целом, его частей и офисной техники.
2). Безопасность информации на автоматизированном рабочем месте врача.
3). Защита информации в медицинской организации на уровне персонального компьютера.
4). Аппаратные средства пользователя информации в медицинском учреждении.
5). Аппаратные средства с ЭВМ различных медицинских организаций.
6). Требования к ЭВМ диагностической аппаратуры.
7). Требования к ЭВМ терапевтической аппаратуры.
8). Требования к ЭВМ хирургической аппаратуры.
9). Информационная безопасность на сетевом уровне.
10). Видео и аудио наблюдение, и видео и аудиорегистрация в медицинской организации.

3.1.3. Контролируемый раздел дисциплины «Обеспечение информационной безопасности в медицинской организации на программном уровне»

Темы рефератов

1). Системы и прикладные программы, используемые в медицинских организациях.
2). Безопасность баз данных и СУБД в медицинских организациях.
3). Безопасность МИС и ЕГИС.
4). Безопасность системы поддержки принятия решений.
5). Безопасность программного обеспечения диагностической, терапевтической, хирургической аппаратуры.
6). Безопасность сетевого программного обеспечения.
7). Компьютерные вирусы их разновидности и борьба с ними.
8). Невирусное вредоносное ПО, его разновидности и борьба с ним.
9). Безопасность информации на уровне мобильных технологий.
10). Безопасность программных продуктов, разработанных в медицинской организации.

3.1.4. Контролируемый раздел дисциплины «Обеспечение информационной безопасности на уровне информационной политики медицинской организации»

Темы рефератов

1). Информационная политика медицинской организации.
2). Обзор информации, к которой разрешён и запрещён доступ пациентам.
3). Обзор информации, к которой разрешён и запрещён доступ докторам и их руководству.
4). Обзор информации, к которой разрешён и запрещён доступ третьим лицам.
5). Обзор медицинских данных разрешённых и запрещённых для публикации в средствах массовой информации.
6). Безопасность медицинской информации на уровне интернет и социальных сетей.
7). Биометрические устройства доступа в медицинской организации.
8). Оценка рисков и меры по их уменьшению в медицинских организациях.
9). Управление системой безопасности в медицинской организации.
10). Государственная тайна, коммерческая тайна, врачебная тайна.

3.2.**Промежуточный контроль**

Вопросы для зачёта

1). Модели нарушителей безопасности информации в медицинской организации.
2). Законодательная защита информации в медицинском учреждении РФ.
3). Мировой опыт в законодательной защите информации в медицине.
4). Предполагаемые последствия от потери, искажения, подлога и несанкционированного копирования медицинской информации.
5). Обзор методов и способов защиты информации от потери.
6). Обзор методов и способов защиты информации от искажения

7). Обзор методов и способов защиты информации от подлога.
8). Обзор методов и способов защиты информации от несанкционированного копирования.
9). Особенности медицинской информации, подлежащей защите.
10). Защита данных при обмене информацией между медицинскими организациями.
11). Работоспособность персонального компьютера в целом, его частей и офисной техники.
12). Безопасность информации на автоматизированном рабочем месте врача.
13). Защита информации в медицинской организации на уровне персонального компьютера.
14). Аппаратные средства пользователя информации в медицинском учреждении.
15). Аппаратные средства с ЭВМ различных медицинских организаций.
16). Требования к ЭВМ диагностической аппаратуры.
17). Требования к ЭВМ терапевтической аппаратуры.
18). Требования к ЭВМ хирургической аппаратуры.
19). Информационная безопасность на сетевом уровне.
20). Видео и аудио наблюдение, и видео и аудиорегистрация в медицинской организации.
21). Системы и прикладные программы, используемые в медицинских организациях.
22). Безопасность баз данных и СУБД в медицинских организациях.
23). Безопасность МИС и ЕГИС.
24). Безопасность системы поддержки принятия решений.
25). Безопасность программного обеспечения диагностической, терапевтической, хирургической аппаратуры.
26). Безопасность сетевого программного обеспечения.
27). Компьютерные вирусы их разновидности и борьба с ними.
28). Невирусное вредоносное ПО, его разновидности и борьба с ним.
29). Безопасность информации на уровне мобильных технологий.
30). Безопасность программных продуктов, разработанных в медицинской организации.
31). Информационная политика медицинской организации.
32). Обзор информации, к которой разрешён и запрещён доступ пациентам.
33). Обзор информации, к которой разрешён и запрещён доступ докторам и их руководству.
34). Обзор информации, к которой разрешён и запрещён доступ третьим лицам.
35). Обзор медицинских данных разрешённых и запрещённых для публикации в средствах массовой информации.
36). Безопасность медицинской информации на уровне интернет и социальных сетей.
37). Биометрические устройства доступа в медицинской организации.
38). Оценка рисков и меры по их уменьшению в медицинских организациях.
39). Управление системой безопасности в медицинской организации.
40). Государственная тайна, коммерческая тайна, врачебная тайна.

Тестовые вопросы

Тестовые вопросы и варианты ответов	*Компетенция, формируемая тестовым вопросом*
1. К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА НЕ ОТНОСИТСЯ: 1) государственная тайна 2) размер золотого запаса страны 3) персональные данные	ПК-2

4) коммерческая тайна	
2 ЕСЛИ РАЗЛИЧНЫМ ГРУППАМ ПОЛЬЗОВАТЕЛЕЙ С РАЗЛИЧНЫМ УРОВНЕМ ДОСТУПА ТРЕБУЕТСЯ ДОСТУП К ОДНОЙ И ТОЙ ЖЕ ИНФОРМАЦИИ, КАКОЕ ИЗ УКАЗАННЫХ НИЖЕ ДЕЙСТВИЙ СЛЕДУЕТ ПРЕДПРИНЯТЬ РУКОВОДСТВУ: 1) снизить уровень классификации этой информации 2) улучшить контроль за безопасностью этой информации 3) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации 4) нет правильного варианта	ПК-2
3. СВОЙСТВО ИНФОРМАЦИИ, НАИБОЛЕЕ АКТУАЛЬНОЕ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: 1) целостность информации 2) доступность информации 3) актуальность информации 4) срочность информации	ПК-7
4. КОГДА ПОЛУЧЕН СПАМ ПО E-MAIL С ПРИЛОЖЕННЫМ ФАЙЛОМ, СЛЕДУЕТ: 1) Прочитать приложение, если оно не содержит ничего ценного – удалить 2) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама 3) Удалить письмо с приложением, не раскрывая (не читая) его 4) Нет правильного варианта	ПК-7
5. УКАЖИТЕ КАТЕГОРИЮ, КОТОРАЯ ЯВЛЯЕТСЯ НАИБОЛЕЕ РИСКОВАННОЙ ДЛЯ КОМПАНИИ С ТОЧКИ ЗРЕНИЯ ВЕРОЯТНОГО МОШЕННИЧЕСТВА И НАРУШЕНИЯ БЕЗОПАСНОСТИ: 1) Хакеры 2) Контрагенты 3) Сотрудники организации	ПК-2
6. ИНФОРМАЦИЯ, КОТОРУЮ СЛЕДУЕТ ЗАЩИЩАТЬ (ПО НОРМАТИВАМ, ПРАВИЛАМ	ПК-2

ИНФОРМАЦИОННОЙ СИСТЕМЫ) НАЗЫВАЕТСЯ: 1) Регламентированной 2) Правовой 3) Защищаемой 4) Ограниченной	
7. КАКИЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЯВЛЯЮТСЯ ПРЕДНАМЕРЕННЫМИ? 1) ошибки персонала 2) открытие электронного письма, содержащего вирус 3) не авторизованный доступ к информации или информационной системе 4) все ответы правильные	ПК-2
8. РАЗНОВИДНОСТЯМИ УГРОЗ БЕЗОПАСНОСТИ (СЕТИ, СИСТЕМЫ) ЯВЛЯЮТСЯ: 1) Программные, технические, организационные, технологические 2) Серверные, клиентские, спутниковые, наземные 3) Личные, корпоративные, социальные, национальные	ПК-2
9. ПОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПОНИМАЕТСЯ… 1) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре. 2) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия 3) нет правильного ответа 4) все ответы правильные	ПК-2
10. ЗА НАРУШЕНИЯ ЗАКОНОДАТЕЛЬСТВА РФ	ПК-2

О ГТ ПРЕДУСМАТРИВАЕТСЯ (...) ОТВЕТСТВЕННОСТЬ 1) уголовная и административная 2) гражданско-правовая 3) дисциплинарная 4) все ответы правильные 5) нет правильного варианта	
11. ЧАСТЬЮ КАКОЙ, БОЛЕЕ ОБЩЕЙ СИСТЕМЫ, ЯВЛЯЕТСЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ? 1) системы защиты национальных интересов страны 2) системы обороны страны 3) системы защиты прав граждан страны 4) системы обеспечения национальной безопасности страны	ПК-2
12. В ЧЕМ ЗАКЛЮЧАЕТСЯ СУЩНОСТЬ ПРИЕМА, ОБЕСПЕЧИВАЮЩЕГО НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ИЗВЕСТНОГО КАК "УБОРКА МУСОРА"? 1) это метод получения информации, хранящейся на жестком диске ПК 2) это метод получения информации, переданной пользователем ПК по модему 3) это метод получения информации, хранящейся на сервере 4) это метод получения информации, оставленной пользователем в памяти ПК после окончания работы	ПК-7
13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАВИСИТ ОТ СЛЕДУЮЩЕГО: 1) компьютеров, поддерживающей инфраструктуры 2) пользователей 3) информации	ПК-2
14. ЗАЩИТА ИНФОРМАЦИИ – ЭТО.. 4) комплекс мероприятий, направленных на обеспечение информационной безопасности.	ПК-7

5) процесс разработки структуры базы данных в соответствии с требованиями пользователей 6) небольшая программа для выполнения определенной задачи 7) все ответы правильные 8) нет правильного ответа	
15. КОНФИДЕНЦИАЛЬНОСТЬ – ЭТО.. 1) защита от несанкционированного доступа к информации 2) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов 3) описание процедур	ПК-2
16. ПО ОТНОШЕНИЮ К ПОДДЕРЖИВАЮЩЕЙ ИНФРАСТРУКТУРЕ РЕКОМЕНДУЕТСЯ РАССМАТРИВАТЬ СЛЕДУЮЩИЕ УГРОЗЫ: 1) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности 2) обрабатывать большой объем программной информации 3) нет правильного ответа 4) все ответы правильные	ПК-7
17. ПОБОЧНОЕ ВЛИЯНИЕ – ЭТО… 1) негативное воздействие на систему в целом или отдельные элементы 2) нарушение работоспособности какого-либо элемента системы вследствие чего функции выполняются неправильно в заданный момент 3) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций	ПК-7
18. КАКИЕ ЛИЦА РАССМАТРИВАЮТСЯ В КАЧЕСТВЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ? 1) поставщики программного обеспечения автоматизированных систем.	ПК-2

2) разработчики программного обеспечения автоматизированных систем. 3) хакеры. 4) лица, имеющие доступ к работе со штатными средствами автоматизированных систем.	
19. ИНФОРМАЦИЮ С ОГРАНИЧЕННЫМ ДОСТУПОМ ДЕЛЯТ: 1) государственную тайну 2) конфиденциальную информацию 3) достоверную информацию	ПК-2
20. УКАЖИТЕ ПОРЯДОК ДЕЙСТВИЙ ПРИ НАЛИЧИИ ПРИЗНАКОВ ЗАРАЖЕНИЯ КОМПЬЮТЕРА. 1__ Сохранить результаты работы на внешнем носителе. 2__ Отключиться от глобальной или локальной сети. 3__ Запустить антивирусную программу.	ПК-7
21. ВРЕДОНОСНАЯ ПРОГРАММА, КОТОРАЯ ПОДМЕНЯЕТ СОБОЙ ЗАГРУЗКУ НЕКОТОРЫХ ПРОГРАММ ПРИ ЗАГРУЗКЕ СИСТЕМЫ, НАЗЫВАЕТСЯ... 1) загрузочный вирус 2) макровирус 3) троян 4) файловый вирус	ПК-7
22. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ – ЭТО… 1) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации 2) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных 3) нет правильного ответа 4) все ответы правильные	ПК-2
23. НАУКА, ЗАНИМАЮЩАЯСЯ ЗАЩИТОЙ ИНФОРМАЦИИ, ПУТЕМ ПРЕОБРАЗОВАНИЯ	ПК-7

ЭТОЙ ИНФОРМАЦИИ ЭТО: 1) криптография 2) криптология 3) криптоанализ	
24. МОЖНО ЛИ ОТНЕСТИ СЛАБУЮ АУТЕНТИФИКАЦИЮ К ПРОБЛЕМАМ БЕЗОПАСНОСТИ? 1) нет 2) да 3) в редких случаях	ПК-7
25. АУТЕНТИФИКАЦИЯ БЫВАЕТ: 1) статическая 2) устойчивая 3) постоянная 4) все варианты правильные 5) правильного варианта нет	ПК-7
26. ВРЕДОНОСНАЯ ПРОГРАММА - ЭТО… 1) программа, специально разработанная для нарушения нормального функционирования систем 2) упорядочение абстракций, расположение их по уровням 3) процесс разделения элементов абстракции, которые образуют ее структуру и поведение	ПК-7
27. К ВРЕДОНОСНЫМ ПРОГРАММАМ ОТНОСЯТСЯ: 1) потенциально опасные программы 2) вирусы, черви, трояны 3) шпионские и рекламные программы 4) вирусы, программы-шутки, антивирусное программное обеспечение 5) межсетевой экран, брандмауэр	ПК-7
28. ОТМЕТЬТЕ СОСТАВНЫЕ ЧАСТИ СОВРЕМЕННОГО АНТИВИРУСА 1) модем 2) принтер 3) сканер 4) межсетевой экран 5) монитор	ПК-7
29. КОМПЬЮТЕРНЫЕ ВИРУСЫ – ЭТО:	ПК-7

1) Вредоносные программы, наносящие вред данным. 2) Программы, уничтожающие данные на жестком диске 3) Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы. 4) Программы, заражающие загрузочный сектор дисков и препятствующие загрузке компьютера 5) Это скрипты, помещенные на зараженных интернет-страничках	
30. К БИОМЕТРИЧЕСКОЙ СИСТЕМЕ ЗАЩИТЫ ОТНОСЯТСЯ: 1) защита паролем 2) физическая защита данных 3) антивирусная защита 4) идентификация по радужной оболочке глаз 5) идентификация по отпечаткам пальцев	ПК-2, ПК-7

Эталоны ответов

Номер тестового задания	*Номер эталона ответа*
1	2
2	2
3	1
4	3
5	3
6	3
7	3
8	1
9	1
10	1
11	4
12	4

13	1
14	1
15	1
16	1
17	1
18	4
19	12
20	231
21	1
22	1
23	2
24	2
25	4
26	1
27	123
28	345
29	3
30	45